1. Contact Information

Department of State Privacy Coordinator
Sheryl Walter
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

a. **Date PIA was completed:** November 26, 2013

b. **Name of system:** IIP Content Management System

c. **System acronym:** CMS

d. **IT Asset Baseline:** (ITAB) number: 600

e. **System description** (Briefly describe scope, purpose, and major functions):

The **Content Management System** is an umbrella grouping of multiple subsystems. The multiple subsystems are built on a variety of cloud computing models: Infrastructure-As-A-Service (IaaS), Platform-As-A-Service (PaaS), and Software-As-A-Service (SaaS). There is no central repository of an individual user's profile data. Each subsystem supports separate disconnected user accounts. The Content Management System supports programs managed by the U.S. Department of State's Bureau of International Information Programs (IIP), in particular, those programs involved with the dissemination of information from the Department to foreign audiences. Content Management System is composed of the following thirteen (13) subsystems:

- **Hosting**

  Hosted at CenturyLink data center in Virginia, this subsystem includes: Linux servers, Windows servers, firewalls, Internet Service Provider, Akamai content distribution network, and IIP Digital website. Authentication is performed via Public/Private Key managed by Century Link.

- **WebGUI**

  WebGUI supports 500+ websites for embassies and consulates, and InfoCentral website, and HumanRights.gov. Authentication is performed via Lightweight Directory Access Protocol (LDAP).

- **RT Ticketing**

  RT Ticketing supports a Help Desk that is operated 24x7x365. Help Desk is a trouble-ticket system dedicated to the IIP/CSS/CMS systems, in particular to the Content Management System hosting every embassy website, consulate website and "virtual presence post" in the U.S. Department of State. The Help Desk serves as a way to measure performance of the IIP/CSS/CMS team's Help Desk staff, offering metrics related to the team's service-level agreement and customer satisfaction. Authentication is performed via the application (a separate account is created in the application).

- **Media Management Tool (MMT)**

  MMT supports the photography assets and metadata. Authentication is performed via LDAP and the application (a separate account is created in the application).

- **MYCMS**

  MYCMS supports user access to libraries of Website promotional badges (i.e. images/banners not personal badges), reports and optional assets. PII is not included in the badges, reports or assets. Authentication is performed via LDAP.

- **WordPress**

  WordPress blogs for Public Diplomacy (PD) outreach to foreign audiences. Authentication is performed via the application (a separate account is created in the application for those updating the content).

  The Young African Leaders Initiative (YALI) web page is the only subsystem that collects PII from individuals who wish to learn more about the Washington Fellowship for Young African Leaders. Information about the initiative is automatically sent when it is available, and the PII cannot be retrieved by anyone using the system or via a search.

- **Google Search Appliance (GSA)**

  Crawls every HTML page for keywords, and responds to search queries from browsers. No PII is collected during the HTML page search (Crawls) or responses to search queries. Authentication is performed via the application (a separate account is created in the application).

- **DataHarmony**

  DataHarmony supports taxonomy searching. Authentication is performed via the application (a separate account is created in the application).

- **WebTrends**

  Provides statistical reports about the usage and visits to each HTML page. No PII is collected or presented in these statistical reports. Authentication is performed via the application (a separate account is created in the application).

- **Google Analytics**

  Provides statistical reports about the usage and visits to each HTML page. No PII is collected or presented in these statistical reports. Authentication is performed via the application, which is externally hosted.

- **Video Studio**

  This application supports the video assets and metadata and it is tied to the YouTube accounts. Authentication is performed via LDAP.

- **Redmine**

  Redmine contains the documentation of the software developer’s efforts with defects and remedies to source code. Authentication is performed via LDAP and the application (a separate account is created in the application).

- **Git Repository**

  Git Repository stores the source code developed by IIP/CSS software developers. Authentication is performed via Redmine and only developers have access to Git Repository.

f. Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

g. Explanation of modification (if applicable): Not applicable.

h. Date of previous PIA (if applicable): February 4, 2008 - it concluded under the old guidelines that no PII existed inside CMS; however the new guidelines (5 FAM 466(a)) widened the PIA requirement to include Department employees.

3. Characterization of the Information

The system:

☐ Does NOT contain Personally Identifiable Information.

☒ Does contain Personally Identifiable Information.

a. What elements of Personally Identifiable Information (PII) are collected and maintained by the system? What are the sources of the information?

The following elements of PII are collected via the new user request form (CMS Account Request Form (CMSARF)) from Department staff (to include full-time employees and contractors):

- User's Name (First MI Last)
- User's Email Address (Government / business only)
- User's Telephone (Government / business)
- User's Office/Bureau & City (ex. IIP, Washington)
- User's Title

Several subsystems (RT Ticketing, Media Management Tool, MYCMS, Redmine) utilize the Government Email Address as the username/ID.

The following elements of PII are collected from individuals requesting information about the President's Young African Leaders Initiative (YALI).

- First and Last Name
- Email Address
- Country

b. How is the information collected?

For the RT Ticketing subsystem, the contact data (point-of-contact information) is either entered into the system by the individuals themselves (i.e. in their signature block as part of their email to Help Desk requesting help) or it is entered by U.S. Department of State staff in support of the end user and obtained from information in the Department's global address list or it is entered via the CMS Access Request Form (CMSARF), which is used to request a new individual user account.

Individuals requesting information about the YALI program provide their contact information via the (Contact Us) web page on the YALI blog.

c. Why is the information collected and maintained?

The PII collected via the CMSARF is used to establish a user account based on their role (i.e. end user, admin, etc.) and is maintained as long as the account is active.

The PII collected via the YALI web page (Contact Us) is used to send information regarding the YALI program.

d. How will the information be checked for accuracy?

Information is collected directly from the record subject and is presumed to be accurate, or from Department of State records which the individual has the ability to review and change for accuracy.

The information collected from the YALI record subject is presumed to be accurate. Subscribers to YALI cannot modify their contact information, but they can send a response to have their information modified or they can simply unsubscribe. The list (listserv) is only scrubbed for duplicates.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 5 U.S.C. 301 (Management of the Department of State);
- 22 U.S.C. 1431 et seq. (Smith-Mundt);
- United States Information and Educational Exchange Act of 1948, as amended;
- 22 U.S.C. 2451-58 Fulbright-Hays Mutual Educational and Cultural Exchange Act of 1961, as amended;
- 22 U.S.C. 2651 a (Organization of the Department of State); and
- 22 U.S.C. 3921 (Management of the Foreign Service).

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

A potential risk is the improper use of business contact information for unofficial or personal use. The PII collected in the system is the minimum amount of information necessary to be able to contact the subject individual for official business purposes or for providing feedback regarding the YALI program.

4. Uses of the Information

a. Describe all uses of the information.

The PII is collected and maintained to provide the authorized user/helpdesk support with a means to contact the subject individual or submitter (i.e. content provider, helpdesk requester) if needed or for providing feedback regarding the YALI program.

b. What types of methods are used to analyze the data? What new information may be produced?

No analysis of the PII is performed and no new PII is produced within the system.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Content Management System does not use commercial information, publicly available information, or information from other Federal agency databases.

d. Are contractors involved in the uses of the PII?

Contractors and the service provider (CenturyLink datacenter located in Sterling, VA) are involved with the operational maintenance of the system. The service provider does not have access to the PII. The contractors use the data in the Content Management System consistent with the statutory purposes, and do not produce any additional data. Privacy Act contract clauses are inserted in their contracts and other regulatory measures are addressed. Rules of Behavior have been established and training regarding the handling of PII under the Privacy Act of 1974 is conducted.

Contractors are employed by the U.S. Department of State within the Bureau of International Information Programs (IIP) as members of staff to support Bureau programs. All contractors, whether technical or direct program support, must pass a government background check prior to having system access. Annual, recurring security training is practiced and conducted through Diplomatic Security.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

PII collected and maintained by the Content Management System is used only for purposes related to the Content Management System Program and to IIP internal task assignments. The information is not analyzed or disseminated for any other purpose. Content Management System does not utilize features that might initiate a functional vulnerability creep or threat.

Authorized employees are assigned level-of-access roles based on their job functions. Roles limit the update capabilities to those deemed necessary for specified job functions.

5. Retention

a. How long is information retained?

Records in Content Management System will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with published record schedules (see below) of the Department of State and as approved by the National Archives and Records Administration.

Record Schedule #	Record Title/ (Disposition)
A-37-008-01	CMS (Content Management System) Training Files (Destroy/delete when updated or superseded.);
A-37-008-03	Schedule of Daily Activities

	(Destroy or delete when no longer needed for convenience of reference.);
A-37-008-05	Customer Service Files (Destroy/delete when 1 year old or when no longer needed for review and analysis, whichever is later.);
A-37-008-06a	Oversight and Compliance Files (Destroy/delete when 5 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer.);
A-37-008-07	System Backups and Tape/File Library Records (Delete backup tapes when superseded or when no longer needed for system restoration, whichever is later.);
A-37-008-08	Files Related to Maintaining the Security of Systems and Data (Destroy/delete 1 year after system is superseded.);
A-37-008-09	User Identification, Profiles, Authorizations, and Password Files (Destroy/delete inactive file 2 years after user account is terminated or password is altered.);
A-37-008-10b	CMS Operations Records (Destroy/delete when 1 year old.);
A-37-008-12	CMS Design and Implementation Files (Destroy/delete 3 years after final decision on acceptance is made.),

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

A potential risk may occur when there is out-dated contact information directly in the Content Management System. This risk is mitigated through periodic guidance that instructs individuals maintain their contact information. Potential privacy risks are mitigated through the publication of the record schedules listed in section 5(a).

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

No PII is internally shared. Government / business only contact information is used to contact the subject individual or submitter if needed.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

No information is transmitted or disclosed; therefore, no safeguards are in place.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

No internal sharing and disclosure occurs; therefore, no risks have been identified.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

No PII is externally shared. Consumers/Visitors to the website cannot retrieve any end user's information/user ID via a normal search routine.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

No information is transmitted or disclosed outside the Department; therefore, no safeguards are in place.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

No external sharing and disclosure occurs; therefore, no risks have been identified.

8. Notice

The system:

☒ Contains information covered by the Privacy Act.

Provide number and name of each applicable system of records.

State-79, Digital Outreach and Communication

☐ Does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Records are not retrieved within CMS by a personal identifier therefore the requirements of the Privacy Act do not apply.

b. Do individuals have the opportunity and/or right to decline to provide information?

Collection of information is voluntary; however, if not provided, access to the system cannot be established or information about the YALI program cannot be provided.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Use of the information is limited to allow users to contact other users. Further limitations may not be exercised by users.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is not provided on the CMSARF as information collected by Content Management System is not covered by the Privacy Act, but by the Department guidelines.

A link to the Department's privacy notice is available in the footer of the YALI website including the Contact Us webpage.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Individuals maintain their contact information. They provide their information initially via the CMS Access Request Form (CMSARF), which is required prior to receiving a user account. If their contact information needs to be updated, another CMSARF is submitted to the help desk (embassy-help@getusinfo.com) with the necessary changes. The Help Desk updates the information in CMS..

In addition, each post is contacted annually to renew and confirm their current user information. At that time, the records in all of the appropriate systems (CMS, MMT, and MyCMS) are updated.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

Notification and redress are not applicable as information collected by Content Management System is not covered by the Privacy Act.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

For all Content Management System (CMS) subsystems, the respective system functional administrators determine, based on approval from a requester's manager, who may be granted access to the system and at what level. The level of access and capabilities permitted are restricted by the role assigned to each individual user. Some users are granted read-only access if they have no need to update system records. Some users are granted access to a particular Content Management System subsystem but not granted access to another subsystem. The separation of roles with different access privileges is in accordance with NIST Special Publication 800-53.

All authorized staff using the system must comply with the Department of State's general "appropriate use policy for information technology". Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e[9]) and OMB Circular A-130, Appendix III.

The security controls in the system are reviewed when significant modifications are made to the system, but at least every three years.

Access to Content Management System is restricted to authorized Department of State personnel who need to use the system as part of their work requirement. Only personnel with an approved ID and password to login to the Content Management System's CenturyLink portal can make select updates to the respective child system.

Department of State system users must pass a government background check prior to having system access. At a minimum, they must possess a security clearance level of confidential, with secret preferred. Annual, recurring security training is practiced and conducted through Diplomatic Security.

Authorized user login identifiers are appended to any system records created or updated. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system.

Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of State systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

SSO is not in place, so to access the different subsystems requires multiple logons (see 2(e) above for authentication process for each system).

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed or attempted to perform on an information system.)

b. **What privacy orientation or training for the system is provided authorized users?**

Annual, recurring security training is practiced and conducted through the Bureau of Diplomatic Security and includes information on protecting PII.

c. **Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.**

The Assessment and Authorization (A&A) process independently verifies and validates the application system security controls. Administrative procedures, including independent security investigations of Department applicants and assignment of unique system access rights to individuals, limit access to the system.

Potential risks exist for administrators to improperly provide access for employees without a need-to-know or to grant excessive permissions to a user. However, there is little residual risk related to access, in particular because the system is available only to Department of State personnel who are expected to comply with the Rules of Behavior for protecting PII.

11. Technologies

a. **What technologies are used in the system that involves privacy risk?**

There are no technologies used that may cause privacy risk.

b. **Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.**

There are no technologies used that may cause privacy risk.

12. Security

a. **What is the security Assessment and Authorization (A&A) status of the system?**

Content Management System is actively in the process of submitting the necessary documentation for the triennial A&A as a Low Risk, High Cost system. The A&A is expected to be granted in December 2013. The ATO was granted on July 23, 2010.